(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 June 2005 (30.06.2005)

PCT

(10) International Publication Number
WO 2005/060153 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number:
PCT/IB2004/052672

(22) International Filing Date: 6 December 2004 (06.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03104686.5 15 December 2003 (15.12.2003) EP

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N. V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SCHOLZE, Steffen** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(74) Agents: **VOLMER, Georg** et al.; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

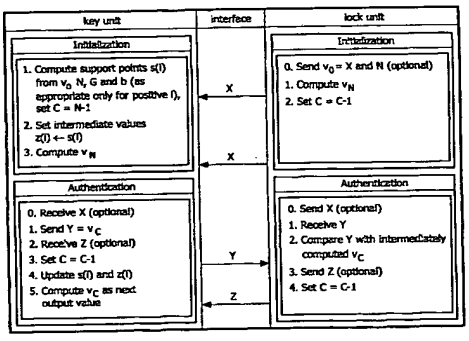
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: USE-AUTHORIZATION DEVICE FOR SECURITY-RELATED APPLICATIONS



(57) Abstract: This description is given of a use-authorization device for security-related applications, in particular access control to secure areas or securing vehicles with a useroperated key unit for generating consecutive, alternating user code information which exhibits a sequence of consecutive function values $v_{i+1} = F(v_i, const)$ for $i = 0,\ldots, N$ through the repeated use of a one-way function $F(v_i, const)$, which function values are used in inverse order to the sequence formation to create the consecutive user code information, and an application-sided processing unit for determining actual authorization information which is dependent upon the user code information received from the key unit and for performing a use-authorization checking process by comparing this actual authorization information with target authorization information saved in the application, as well as for generating use-release information depending on the result of the comparison, wherein the target authorization information has a function value v; which has been transferred from the user code information processed during the previous positive use-authorization operation. The special feature of the invention is that there is a certain number of levels G provided, with at least one support point and one intermediate value, from which a certain number of iterative function value calculations can be performed in each level by means of the one-way function $F(v_i, const)$wherein there are $G = L(N) / b$levels, with N as the starting value, $L(N)$ as the number of bits required for representing N in the dual system and b as the basis.

WO 2005/060153 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.